

5 FAH-11 H-500 PERFORMANCE MEASURES FOR INFORMATION ASSURANCE

5 FAH-11 H-510 GENERAL

(CT:IAH-3; 03-26-2007)
(Office of Origin: IRM/IA)

5 FAH-11 H-511 INTRODUCTION

5 FAH-11 H-511.1 Purpose

(CT:IAH-3; 03-26-2007)

- a. This subchapter implements the policy in 5 FAM 1060 (Information Assurance Management). It addresses the requirement that Federal agencies collect and report performance metrics and measures for Department programs, including information assurance, to demonstrate compliance with laws and regulations, improve accountability for their programs, and advance efficiencies in delivering programs and services. As required by the Government Performance Results Act (GPRA) and the Clinger-Cohen Act, the Department must ensure that performance measurements are prescribed for Information Technology (IT) used by, or to be acquired for, the Department. In addition, these measurements must indicate how well the IT supports the Department's programs (see 40 U.S.C. 11313(3); see also 31 U.S.C. 1115(a)).
- b. These procedures also explain how system owners and managers must work together to ensure that performance metrics are applied for Department information technology (IT) personnel who are assisting in developing, implementing, and managing an IT security program.
- c. Current Federal requirements relating to IT security performance measures require a formalized process on how an agency, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures.
- d. National Institute of Standards and Technology (NIST) Special Publications (SP) 800-26, Revision 1, NIST SP 800-53, and NIST SP 800-

80 identify management, operational, and technical control topic areas that affect the security posture of an IT system. This subchapter provides a recommended methodology for quantifying the critical elements in NIST SPs 800-26, 800-53, and 800-80 for monitoring and reporting on implementation and effectiveness of the system security controls.

5 FAH-11 H-511.2 Definitions

(CT:IAH-3; 03-26-2007)

Performance Measures: Evaluation benchmarks that facilitate decision making and accountability through collection, analysis, and reporting of relevant performance data. They provide relevant trends over time and are useful in tracking performance and directing resources to initiate performance improvement actions.

Performance Metrics: A set of standard measures used to identify and evaluate how well specified characteristics or properties of resources, processes, customers, or desired results change over time when compared against a baseline value.

5 FAH-11 H-511.3 Objective

(CT:IAH-3; 03-26-2007)

- a. The objective of this subchapter is to provide a comprehensive, uniform approach to developing, implementing, and managing performance measures as they pertain to information assurance at the system level.
- b. Understanding the following concepts is vital to improving the effectiveness of measuring performance at the system level:
 - (1) IT security measures provide a practical approach to assessing information security at the system level through collecting, analyzing, and reporting relevant performance data.
 - (2) Based on IT security performance goals and objectives, IT security metrics must be quantifiable, measurable, readily collectible, and repeatable. They provide relevant trends over time and are useful in tracking performance, facilitating decision making, and directing resources to initiate performance improvement actions.
 - (3) System or user-level performance measures are linked to agency measures, which are linked to the Federal mandate for performance measures for information assurance, thereby creating a pyramid of measures that range from tactical to operational to strategic. (See the Department's Information Security Program Plan (ISPP) on the Office of Information Assurance (IRM/IA) Web site; the specific link

is shown as Management Plan).

- (4) The use of performance measures and the data they reveal support overall management of the IT system over its lifecycle.
- (5) Metrics improve accountability to stakeholders, ensure an appropriate level of mission support, determine IT security program effectiveness, and demonstrate program impact to Department management.

5 FAH-11 H-511.4 Scope

(CT:IAH-3; 03-26-2007)

- a. This subchapter focuses on how to establish, apply, and maintain information security performance measures at the system level. It also discusses how to develop effective performance measures for capturing the elements in the Information Security Program Plan (ISPP) and to ensure compliance with Department IT performance measures, policies, and security controls (see 5 FAM 130).
- b. This subchapter does not include specifics related to agency-level performance measures. However, system-level metrics do support agency-level reporting on progress towards achieving strategic goals (see 5 FAM 671).
- c. IRM/IA is responsible for the content of this subchapter. If there are any questions, please e-mail IRM/IA.

5 FAH-11 H-511.5 Authorities

(CT:IAH-3; 03-26-2007)

- a. Federal Information Security Management Act (FISMA) (Public Law 107-347, Title III), December 2002.
- b. Paperwork Reduction Act (PRA) of 1995 (Public Law 104-13), May 1995.
- c. The Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)), also known as the Information Technology Management Reform Act.
- d. Government Performance and Results Act of 1993 (GPRA) (Public Law 103-62).
- e. Government Paperwork Elimination Act (GPEA) (44 U.S.C. §3504).
- f. NIST Standards and Special Publications (SPs):
 - (1) SP 800-26, Revision 1, Security Self-Assessment Guide for Information Security Program Assessments and System Reporting Form, August 2005;
 - (2) SP 800-53, Revision 1, Recommended Security Controls for Federal

Information Systems, December 2006;

- (3) SP 800-55, Security Metrics Guide for Information Technology Systems, July 2003;
- (4) SP 800-80, Guide for Developing Performance Metrics for Information Security (draft), May 2006;
- (5) Federal Information Processing Standard 199 (FIPS 199), Standards for Security Categorization of Federal Information and Information Systems, February 2004; and
- (6) Federal Information Processing Standard 200 (FIPS 200), Minimum Security Requirements for Federal Information and Information Systems, March 2006.

5 FAH-11 H-511.6 Roles and Responsibilities

(CT:IAH-3; 03-26-2007)

- a. **The Chief Information Officer (CIO)** has the following responsibilities related to IT security performance measures:
 - (1) Demonstrates through formal leadership management's commitment to the development, implementation, and maintenance of IT security measures;
 - (2) Communicates, formally, the importance of using IT security measures to monitor the overall management of the IT security program and to comply with applicable regulations;
 - (3) Ensures the program development, implementation, and maintenance of IT security performance measures;
 - (4) Allocates adequate financial and human resources to the performance measures program;
 - (5) Communicates with system owners to facilitate metrics acceptance and build support for the program;
 - (6) Directs the collection of performance measures data;
 - (7) Reviews IT security measures regularly and uses data derived from the measures to support policy and budget decisions, better resource allocations, and improved understanding of the IT security posture; and
 - (8) Issues IT security performance measures policies, procedures and guidance.
- b. **The Chief Information Security Officer (CISO)** has the following responsibilities related to IT security performance measures:
 - (1) Leads the Department's program for the development,

implementation, and maintenance of IT security metrics under the direction of the CIO;

- (2) Ensures a standard Department process is used for the development, creation, and analysis of IT metrics;
- (3) Develops policies and procedures related to IT security metrics;
- (4) Obtains adequate staff and financial resources to support program development and implementation of IT metrics;
- (5) Actively solicits input from and provides feedback to system owners, system managers, and security personnel at every step in the development of IT performance metrics;
- (6) Ensures that IT performance metrics data is collected, analyzed, and reported to the CIO and system owners;
- (7) Reviews IT security performance metrics to determine if there is support for policy, resource allocation, and budget decisions, and its impact on the IT security program;
- (8) Educates system owners on utilizing IT security metrics data for policy, resource allocation, and budget decisions;
- (9) Ensures metrics that have reached their performance target are phased out and replaced by new metrics;
- (10) Ensures manageability of the program by limiting the number of collected metrics at a single point in time;
- (11) Analyzes and establishes prioritization of metrics and directs programs to address high priority items and problem areas;
- (12) Ensures that the corrective actions, identified through measuring IT security performance, are implemented; and
- (13) Develops and implements performance metrics in the Department's automated reporting tool as part of the agency-wide FISMA reporting process.

c. **The system owner** has the following responsibilities related to IT security performance measures:

- (1) Identifies performance metrics as part of the IT business case required in Office of Management and Budget (OMB) budget guidance (OMB Circular A-11) and by the Department's Electronic Capital Planning and Investment Control (e-CPIC) process;
- (2) Implements and maintains performance measures to support the management of the IT investment;
- (3) Collects and submits to IRM/IA performance measures data, including the use of the Department's automated reporting tool, for

- tracking compliance actions in support of the agency-wide FISMA reporting process; and
- (4) Collects and reports on systems' metrics as a part of the agency-wide FISMA reporting process and tracks and allocates resources for corrective actions.
- d. **The information system security officer (ISSO)** has the following responsibilities related to IT security performance measures:
- (1) Participates in information security metric program development and implementation by providing feedback on the feasibility of data collection and identification of data sources and repositories;
 - (2) Collects and provides metrics data to designated staff for data analysis and reporting; and
 - (3) Assists with the implementation of corrective actions derived from the measurement and analysis of IT security performance.

5 FAH-11 H-512 ESTABLISHING INFORMATION SECURITY PERFORMANCE MEASURES

5 FAH-11 H-512.1 Performance Measures Essentials

(CT:IAH-3; 03-26-2007)

- a. **Types of Performance Measures:** The type of performance measures used depends on the maturity of the security control implementation in the organization as follows:
- (1) **Implementation measures:** are used when security controls have been defined in procedures and are in the process of being implemented. The metrics are used to demonstrate progress in implementing policies and procedures for individual security controls.
 - (2) **Efficiency measures:** in a more advanced security program efficiency measures are used to assess the timeliness and efficiency of security control implementation.
 - (3) **Impact measures:** as controls become fully implemented and refined impact measures assess the impact of these controls on the Department's strategic missions and goals, often through quantifying the cost savings produced by the security program or through costs incurred from addressing security events.

- b. **Characteristics of Performance Measures:** IT security performance measures should have the following characteristics:
- (1) Quantitative information format (Percentages, averages, and numbers);
 - (2) Supporting data that is readily available and collectible;
 - (3) A repeatable process that can be measured repeatedly over time; and
 - (4) Usefulness to management for tracking performance and directing resources

5 FAH-11 H-512.2 Incorporating Security Controls Into A Security Program Using Performance Measures

(CT:IAH-3; 03-26-2007)

Developing information security performance measures should be a part of a broader process of defining a complete set of performance measures for managing an information security program as noted below:

- (1) As a part of its charter for providing guidance on organizing and managing an information security program, NIST has published SP 800-53 that identifies minimum security controls for Federal information systems. These minimum security controls are organized into 17 security control families (see 5 FAH-11 Exhibit H-512.2.)
- (2) Information security performance measures provide a means for monitoring and reporting an agency's implementation of the SP 800-53 security controls. The performance measures are also used to assess the effectiveness of the security controls in protecting agency information resources in support of the agency's mission.

5 FAH-11 H-513 HOW TO DEVELOP INFORMATION SECURITY PERFORMANCE MEASURES

(CT:IAH-3; 03-26-2007)

The specific aspect of IT security that performance measures will focus on at a given point in time depends on the maturity of the information security program and its success. The sections listed below explain how to develop performance metrics.

5 FAH-11 H-513.1 Create Metrics

(CT:IAH-3; 03-26-2007)

- a. The performance metrics development approach provides two ways of developing metrics, depending on the depth of analysis desired by management:
 - (1) The control-specific approach selects individual controls as the basis for a metric that best represents the entire control family (see 5 FAH-11 Exhibit H-513.1(1)) as determined by the organizational environment; and
 - (2) The cross-cutting approach focuses on metrics that gauge security performance based on more than one individual control or control families (see 5 FAH-11 Exhibit H-513.1(2)). This type of metric provides a broader view of information security performance than the control specific approach.
- b. Deriving the metric for each method of development involves the following methods:
 - (1) In the control-specific method, the selected control and derived metric:
 - (a) Maps directly to an individual control within the respective control family;
 - (b) Uses the data describing the individual control's implementation to generate required metrics such as plan of action and milestones (POA&M), testing, and project tracking; and
 - (c) Characterizes the metric as applicable to low, moderate or high system categorization.
 - (2) In the cross-cutting approach, the metric:
 - (a) Maps to information security goals and objectives that may encompass performance of several information security controls belonging to several control families; and
 - (b) Uses the data from two or more control sources describing the security program's performance to generate the required measurement.

5 FAH-11 H-513.2 Apply Metrics Template

(CT:IAH-3; 03-26-2007)

- a. Organizations should document their performance measures in a standard format (see paragraph b below) to ensure repeatability of metric

development tailoring, collection and reporting processes. A standard format provides detail to guide metrics collection, analysis, and reporting activities.

- b. Examples of control metric templates are shown in 5 FAH-11 Exhibit H-513.2(1) (for a control-specific template) and 5 FAH-11 Exhibit H-513.2(2) (for a cross-cutting control template).

5 FAH-11 H-514 MAINTAINING INFORMATION SECURITY PERFORMANCE MEASURES

5 FAH-11 H-514.1 Collect Data

(CT:IAH-3; 03-26-2007)

- a. The Department's automated FISMA reporting tool is IA-supported and provides systems owners and managers with a mechanism for capturing all of the NIST recommended IT security performance measures, including identification and remediation of POA&MS.
- b. Systems owners may need to develop other tracking tools to document current performance and archive recorded performance measurement data.
- c. Depending on the complexity of the system and the measures selected, a data collection tool may be as simple as an MS Excel spreadsheet or as complex as a custom database with a Web-based front end to display real-time performance measurement information.

5 FAH-11 H-514.2 Meet Reporting Requirements

(CT:IM:03; 03-26-2007)

- a. Timing and format for reporting system security performance measures should support the Department's Corrective Action Plan (CAP), quarterly reporting.
- b. FISMA data calls issued by IRM/IA will prompt system owners to submit information on the status of their IT security performance measures.

5 FAH-11 H-515 THROUGH 519 UNASSIGNED

5 FAH-11 EXHIBIT H-512.2 FAMILIES OF SECURITY CONTROLS

(CT:IAH-3; 03-26-2007)

This exhibit lists the families of controls presented in NIST Special Publication 800-53. It presents the breadth of controls that must be addressed in an Information Assurance Program.

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems), and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT): Organizations must:

- (1) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations or procedures related to the security of organizational information systems; and
- (2) Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability (AU): Organizations must:

- (1) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized or inappropriate information system activity; and
- (2) Ensure that the actions of individual information system users can be uniquely traced to those users so that they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments (CA): Organizations must:

- (1) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application;
- (2) Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;
- (3) Authorize the operation of organizational information systems and any associated information system connections; and
- (4) Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management (CM): Organizations must:

- (1) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and
- (2) Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information

resources and continuity of operations in emergency situations.

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users or devices, and authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response (IR): Organizations must:

- (1) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and
- (2) Track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance (MA): Organizations must:

- (1) Perform periodic and timely maintenance on organizational information systems; and
- (2) Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection (MP): Organizations must:

- (1) Protect information system media, both paper and digital;
- (2) Limit access to information on information system media to authorized users; and
- (3) Sanitize or destroy information system media before disposal or release for reuse.

Physical and Environmental Protection (PE): Organizations must:

- (1) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;
- (2) Protect the physical plant and support infrastructure for information systems;
- (3) Provide supporting utilities for information systems;
- (4) Protect information systems against environmental hazards; and
- (5) Provide appropriate environmental controls in facilities containing information systems.

Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security (PS): Organizations must:

- (1) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions;
- (2) Ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and
- (3) Employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets

and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition (SA): Organizations must:

- (1) Allocate sufficient resources to adequately protect organizational information systems;
- (2) Employ system development life cycle processes that incorporate information security considerations;
- (3) Employ software usage and installation restrictions; and
- (4) Ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Communications Protection (SC): Organizations must:

- (1) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and
- (2) Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity (SI): Organizations must:

- (1) Identify, report, and correct information and information system flaws in a timely manner;
- (2) Provide protection from malicious code at appropriate locations within organizational information systems; and
- (3) Monitor information system security alerts and advisories and take appropriate actions in response.

5 FAH-11 EXHIBIT H-513.1(1) CONTROL-SPECIFIC APPROACH TEMPLATE REQUIREMENTS

(CT:IAH-3; 03-26-2007)

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	As cited in NIST SP 800-53			
Metric ID	Associated control number from SP 800-53			
Strategic Goal or Objective	Agency strategic goal or objective that the metric supports			
Information Security Goal	Statement of requirement or security goal for the metric			
Control	Individual control being measured			
Control Enhancement	Control enhancement, if any, associated with the selected control			
Control Question	Describes what this metric is measuring			
Metric	What is being measured			
Metric Type	Implementation-Effectiveness-Impact			
Frequency of Data Collection	How often the data is collected and analyzed to be reported internally or externally			
Target	Minimum standard for a satisfactory rating for the metric			
Formula	Formula for calculating the metric			
Information Source	The organization(s) or function(s) responsible for collecting the metric data			
Related Control Families	Dependencies for the metric with other control families			
Applicability	Corresponding security categorization for measured control (Low, Moderate, High)			

5 FAH-11 EXHIBIT H-513.1(2) CROSS-CUTTING METRICS DEVELOPMENT APPROACH TEMPLATE REQUIREMENTS

(CT:IAH-3; 03-26-2007)

Cross-Cutting Metrics Development Approach Template	
	Details
Control Families	As cited in NIST SP 800-53
Metric ID	Associated control number from SP 800-53
Strategic Goal or Objective	Agency strategic goal or objective that the metric supports
Information Security Goal	Statement of requirement or security goal for the metric
Control Question(s)	Describes what this metric is measuring
Metric(s)	What is being measured
Metric Type(s)	Implementation-Effectiveness-Impact
Frequency of Data Collection	How often the data is collected and analyzed to be reported internally or externally
Target(s)	Minimum standard for a satisfactory rating for the metric
Formula(s)	Formula for calculating the metric
Information Source	The organization(s) or function(s) responsible for collecting the metric data

5 FAH-11 EXHIBIT H-513.2(1) EXAMPLE OF A CONTROL-SPECIFIC APPROACH TEMPLATE

(CT:IAH-3; 03-26-2007)

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Contingency Planning			
Metric ID	Contingency Plan Testing		X	X
Strategic Goal or Objective	Identify and assess the vulnerability of critical infrastructure and key assets			
Information Security Goal	Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post disaster recovery for Department information systems			
Control	Organizations must test system contingency plans annually to determine the plan's effectiveness and the organization's readiness to execute the plan		X	x
Control Enhancement(s)	(1) The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations		X	X
	(2) The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan			
Control Questions	(1) Did the contingency plan get tested at the alternate processing site?		X	X
	(2) What systems were successfully addressed in the testing of the contingency plan?		X	X
Metric(s)	(1) Percentage of systems successfully testing the contingency plan at the alternate processing site		X	X
	(2) Percentage of systems successfully addressed in the testing of the contingency plan		X	X
Metric Type	Implementation		X	X
Frequency of Data Collection	At least annually		X	X
Target	100 % of High		X	X
Formula	(1) Number of systems tested at the alternate processing site divided by the number of systems in Information Technology		X	X

U.S. Department of State Foreign Affairs Handbook (FAH) Volume 5 Handbook 11 -
Performance Measures for Information Assurance

	Application Baseline (ITAB) (2) Number of systems successfully addressed divided by the number of systems in ITAB			
Information Sources	CIO, IRM/OPS, Computer Incident Response Team (CIRT), CISO, System Owner, ISSO			
Related Control Families	Dependencies for the metric with other control families			
Applicability	Corresponding security categorization for measured control (Low, Moderate, High)		X	X

5 FAH-11 EXHIBIT H-513.2(2) EXAMPLE OF A CROSS-CUTTING METRICS DEVELOPMENT APPROACH TEMPLATE

(CT:IAH-3; 03-26-2007)

Cross-Cutting Metrics Development Approach Template	
	Details
Control Families	Physical and Environmental Protection, Access Control, Incident Response
Metric ID	Unique identifier to be filled out by the organization
Strategic Goal or Objective	Manage IT resources, using e-Gov, to improve service for our customers and partners
Information Security Goal	Integrate physical and information security protection mechanisms to ensure appropriate protection of the organization's IT resources
Control Question(s)	Has the organization implemented appropriate physical security measures to reduce the risks to its IT resources?
Metric(s)	Percentage of physical security incidents allowing unauthorized entry into facilities containing information systems
	Percentage of information security incidents caused by physical access control failures
	Cost of information security incidents of unauthorized access to information systems, due to physical security failures
Metric Type(s)	Effectiveness
	Effectiveness
	Impact
Frequency of Data Collection	Organization defined – (example, monthly report)
	Organization defined – (example, quarterly report)
	Organization defined – (example, quarterly report)
Target(s)	Organization defined – (example zero)
	Organization defined
	Organization defined
Formula(s)	No of physical security incidents allowing unauthorized entry divided by the total number of physical security incidents times 100
	No. of information security incidents due to physical security breaches divided by the total no. of information security incidents times 100

U.S. Department of State Foreign Affairs Handbook (FAH) Volume 5 Handbook 11 -
Performance Measures for Information Assurance

	Sum of costs of each incident within the reporting period
Information Sources	Computer Security Incident Response Team (CIRT); The DS Office of Physical Security (DS/C/PSP)